APPLICATION

of

TERRANCE A. TOMKOW, PHD.

for

UNITED STATES LETTERS PATENT

on

SYSTEM FOR, AND METHOD OF, AUTHENTICATING AN ELECTRONIC MESSAGE TO A RECIPIENT

Client ID/Matter No. RPOST-66232

Sheets of Drawings: Nineteen (19); Figures (1-14)

Express Mail Label No. [EV325905266US]

[31838.1]

Attorneys
FULWIDER PATTON LEE & UTECHT, LLP
Howard Hughes Center
6060 Center Drive, Tenth Floor
Los Angeles, CA 90045

SYSTEM FOR, AND METHOD OF, AUTHENTICATING AN ELECTRONIC MESSAGE TO A RECIPIENT

CROSS-REFERENCE TO RELATED APPLICATION

This application is a non-provisional application corresponding to provisional application 60/429,133 (attorney's file RPOST-62993) filed on November 26, 2002 by Terrance A. Tomkow, for a System For, and Method Of, Authenticating the Transmission and Content of a Reply to an Electronic Message.

This invention relates to a system for, and method of, providing for the transmission of a message by a server to a recipient of a message from a sender and for subsequently providing for the authentication of the message to the recipient. This invention also relates to a system and method whereby a recipient of an electronic message verifies the origination of a received message and knows that the message has not been altered since it was transmitted from the originator.

BACKGROUND OF A PREFERRED EMBODIMENT OF THE INVENTION

In recent years e-mail has become an indispensable business tool. E-mail has replaced "snail mail" for many business practices because it is faster, cheaper and generally more reliable. But there remain some mail applications where hard copy is still dominant, such as registered and certified mail. For example, when a letter is sent by certified mail the sender is provided with a receipt to prove that the letter was mailed. A returned registered mail receipt adds the Postal Service's confirmation that the letter was successfully delivered to the addressee or the addressee's authorized agent. Additionally, private couriers such as Federal Express® and United Parcel Service® (UPS) provide some type of delivery confirmation. Since every piece of

courier mail is, in effect, registered, it is natural for consumers to turn to these services when they want proof of delivery.

Many existing e-mail systems and e-mail programs already provide for some form of proof of delivery. For instance, some e-mail systems today allow a sender to mark a message with "request for notifications" tags. Such tags allow a sender to request notification that the message was delivered and/or when the message was opened. When a sender requests delivery notification, the internet e-mail system may provide the sender with an e-mail receipt that the message was delivered to the mail server or electronic in-box of the recipient. The receipt message may include the title of the message, the destination address, and the time of delivery. It may also include (depending on the types of "flags" that are provided and activated in the mailing software) a list of all the internet "stations" that the message passed through en route to its destination. This form of reporting is built into some of the rules and protocols which implement e-mail. Furthermore, when a message is sent with a "read notification" request, the recipient's e-mail program may send to the sender an e-mail notification that the recipient opened that message for reading. Many electronic mail clients can and do support this kind of reporting; however, internet protocols do not make this mandatory.

However, this does not mean that an e-mail sent with a notification request is as effective in all respects as registered mail. People certify and register letters because they want proof of delivery, e.g., proof that can be used in a civil or criminal proceeding, or proof that will satisfy a supervisor or a client or a government agency that a message has been sent, a job has been done, an order placed, or a contract requirement satisfied.

A registration receipt from the United States Postal Service (USPS) constitutes proof of delivery because the USPS stands behind it. The receipt represents the Post Office's confirmation that the letter or package in question was actually delivered to the addressee or his authorized representative. On the other hand, various hurdles exist

to an e-mail receipt being admitted and relied upon as persuasive evidence in a court of law as a proof that the message was delivered. After all, the receipt may be just another e-mail message that could have been altered or created by anyone, at any time.

There exists a need for an e-mail system and/or method that can provide reliable proof of the content and delivery of an e-mail message in order to take fuller advantage of the convenience and low cost of communicating via e-mail.

To meet this need some systems have been established whereby senders may receive third party proof of delivery by enrolling in services whereby:

a) The sender transmits an electronic message to a third party together with a list of the document's intended recipients.

b) The third party sends a notification to each of the message's intended recipients inviting them to visit the third party's web site where the message can be viewed.

c) If the intended recipient visits the third party's web site to view the message, the third party records this visit so that the sender may know that his message has been read by the recipient.

The drawbacks of such systems are manifold. In the first place, they rely essentially on the co-operation of the recipient of the e-mail to collect his or her messages from the third party's service. But the circumstances in which a sender may want proof of delivery of a message are often ones in which it cannot be assumed that the intended recipient will co-operate in receiving the message. In such cases, e.g. where acknowledging receipt of the message would place a financial or legal burden on the recipient, the recipient can simply ignore the notification that mail is available for him to receive. Note that there is nothing in such a system to guarantee that the intended recipient has received notification of waiting mail. In the second place, such

systems are cumbersome and slow to use as compared to regular e-mail insofar as it can require the sender and/or the recipient to connect to a World Wide Web site to send, collect and verify the delivery of each message. Moreover, transmission of documents by such methods may require both sender and receiver to upload and download files to a web site. Finally, because these methods require the third party to retain a copy of the whole of each message until such time as they are collected or expired, the methods can require its provider to devote substantial computational resources to data storage and data tracking over an extended period of time. As an alternative method of providing proof of delivery, some systems provide proprietary e-mail clients or web-browser plug-ins that will notify senders when a message has been received provided that a recipient uses the same e-mail client. The obvious disadvantage of such systems is that they require both sender and recipient to use the same e-mail client.

Therefore, there exists a need for an e-mail system/method that (1) can provide reliable proof of the content and delivery of electronic messages, (2) which does not require the compliance or co-operation of the recipient, (3) requires no special e-mail software on the part of sender or recipient, (4) operates with the same or nearly the same convenience and speed of use as conventional e-mail, and (5) can be operated economically by a service provider.

In co-pending application 09/626,577 (attorneys file RPOST-57228), filed by Dr. Terrance A. Tomkow and assigned of record to the assignee of record of this application, a system and method are disclosed and claimed for reliably verifying via secure and tamper-proof documentation the content and delivery of an electronic message such as an e-mail. Ideally, the invention disclosed and claimed in co-pending application 09/626,577 (attorneys file RPOST-57228) will give e-mail and other electronic messages a legal status on a par with, if not superior to, that of registered United States mail. However, it is not necessary to the invention that any particular legal status is accorded to messages sent according to the methods taught in

co-pending application 09/626,577, as the invention provides useful information and verification regardless.

The invention disclosed and claimed in co-pending application 09/626,577 includes an electronic message system that creates and records a digital signature of each electronic message sent through the system. An originator may send a copy of the electronic message to the system or generate the electronic message within the system itself. The system then forwards and delivers the electronic message to all recipients (or to the designated message handlers associated with the recipients), including "to" addressees and "cc" addressees. Thereafter, the system returns a receipt of delivery to the originator of the electronic message. The receipt includes, among other things: the original message, the digital signature of the message, and a handshaking and delivery history including times of delivery to the recipients and a digital signature of the handshaking and delivery history. To later verify and authenticate information contained in the receipt, the originator or user sends a copy of the message, the digital signature of the message and the receipt to the system. The system then verifies that the digital signature is the digital signature of the original message. The system then sends a letter or provides other confirmation of authenticity verifying that the electronic message has not been altered.

The receipt may also include a digital signature of the handshaking and delivery history. The system may verify that this digital signature is a digital signature of the handshaking and delivery history. This provides a further verification that the message has not been altered.

The system disclosed and claimed in co-pending application 09/626,577 may include a form of e-mail server connected to the internet, which can be utilized in many ways. For instance, individual users can register their electronic messages, such as e-mails, by sending a "carbon copy" ("cc:") to the system or composing the message within the system itself. For corporate or e-commerce users, these users can change their server to a server incorporating the present invention and have all of their external

electronic messages registered, with the option of having the system retain and archive the receipts. The system can accept and verify encrypted electronic messages and manage the electronic messages within and/or outside a "fire wall." For web-based users, i.e., individuals or corporations using web-based e-mails, such as MSN Hotmail® or Yahoo Mail®, such users could check a box or otherwise set a flag within their e-mail programs to select on a case-by-case basis whether to make the e-mails of record and/or to archive the messages using the system disclosed and claimed in co-pending application 09/626,577.

The digital signature can be created using known digital signature techniques, such as by performing a hash function on the message to produce a message digest and then encrypting the message digest. Separate digital signatures can be created for the body of the message, any attachments, and for the overall message including the body, the attachments, and the individual message digests. The encrypted message digest provides one type of message authentication or validation code, or secure documentation. Other message authentication and/or validation codes may also be generated and used.

In one aspect, the invention disclosed and claimed in co-pending application 09/626,577 is a method of providing proof regarding the delivery and content of an electronic message, comprising: receiving from a sender across a computer network an electronic message, the message having a delivery address associated therewith; computing a message digest according to the message; encrypting the message digest; sending the message electronically to a destination corresponding to the delivery address; recording the Simple Mail Transport Protocol (SMTP) or Extended SMTP (ESMTP) dialog which effects the delivery of the message; receiving Delivery Status Notification information associated with the message and the delivery address; providing to the sender an electronic receipt, the receipt comprising: a copy of the message, the encrypted message digest, the (E)SMTP transcripts, and at least a subset of the Delivery Status notification information, and, at a future date, receiving

electronically the electronic receipt from the sender, verifying that the encrypted message digest corresponds to the message, and verifying that the message was received by an electronic message handler associated with the delivery address.

In another aspect, the invention disclosed and claimed in co-pending application 09/626,577 includes a method of verifying delivery of an electronic message, comprising: in a wide area network computer system, receiving an electronic message from a message sender for routing to a destination address; establishing communication with an electronic message server associated with the destination address, the server defining a destination server; querying the destination server to determine whether the destination server supports Delivery Status Notification (DSN) functionality; receiving a response to the query, the query and response together defining an SMTP dialog; requesting Delivery Status notification information from the destination server according to results of the SMTP dialog; transmitting the electronic message to the destination address; receiving DSN information from the destination server with respect to delivery of the electronic message; and providing to the message sender at least a portion of the SMTP dialog, and at least a portion of the DSN information.

In yet another aspect, the invention disclosed and claimed in co-pending application 09/626,577 includes a method of verifying content of a received electronic message, comprising: receiving the electronic message; generating a digital signature corresponding to the content of the received message; providing the message and the digital signature to a designated addressee; and, at a later time, verifying that the digital signature is the digital signature of the message.

In accordance with still another aspect of the invention disclosed and claimed in co-pending application 09/626,577, the method includes establishing whether a message was electronically received by a recipient, comprising: providing a message to be dispatched electronically along with a recipient's address from a sender; creating a signature associated with the message; dispatching the message electronically to the

recipient's address; tracking the message to determine a final Delivery Status of the message dispatched to the recipient's address; upon receiving final Delivery Status of the message, generating a receipt, the receipt including a copy of the message, the signature, and the final Delivery Status for the message; and providing the receipt to the sender for later establishing that the message was electronically received by the recipient.

In accordance with yet another aspect of the invention disclosed and claimed in co-pending application 09/626,577, a method is provided for proving that an electronic message sent to a recipient was read, comprising: providing an electronic message along with a recipient's address; calculating a digital signature corresponding to the electronic message; dispatching the electronic message electronically to the recipient's address; requesting a Mail User Agent (email client "reading") notification from the recipient; upon receiving the reading notification, generating a reading receipt, the reading receipt including a copy of the message, the digital signature for the corresponding electronic message, and a second digital signature for the reading receipt from the recipient; and providing the reading receipt for later verification that said message was received by the recipient.

The verification discussed in the previous paragraph may be provided by hashing the message to provide a first digital fingerprint and decrypting the digital signature of the message to provide a second digital fingerprint and by comparing the two digital fingerprints. The verification discussed in the previous paragraph may be further provided by hashing the reading receipt from the recipient to provide a third digital fingerprint, by decrypting the digital signature of the reading recipient from the recipient to provide a fourth digital fingerprint and by comparing the third and fourth digital fingerprints.

In accordance with another aspect of the invention disclosed and claimed in co-pending application 09/626,577, a method is provided for validating the integrity of a purported copy of an electronic message, comprising: receiving the purported

electronic message copy, said purported copy including an encrypted message digest associated therewith; decrypting the encrypted message digest; generating a second message digest based on content of the purported copy; and validating the purported copy by comparing the decrypted message digest and the second message digest to determine whether the two message digests match.

In accordance with a still further aspect of the invention disclosed and claimed in co-pending application 09/626,577, a method is provided for validating a received registered e-mail, comprising: receiving an electronic receipt, said receipt including a base message and an encrypted message digest; decrypting the encrypted message digest; generating a second message digest from the base message; and validating the e-mail if the decrypted message digest matches the second message digest.

In yet another aspect, the invention disclosed and claimed in co-pending application 09/626,577 includes a website at which users can go to send and receive secure messages, with the website host acting as an independent third party which will send and receive the messages and provide secure documentation regarding the content and delivery of the messages.

In co-pending application 09/626,577, an authentication of a message provided by a sender to a server and sent by the server to a recipient is provided by the server to the sender. In one embodiment, the server transmits the message to a recipient. The message may pass through intermediate stations before it reaches the recipient. These intermediate stations and the times of the transmission to these intermediate stations are recorded. Other intermediate stations between the recipient and the server provide a record of their operations and the time of their operations in passing all of the information relating to the transmission of the message from the server to the recipient and relating to the transmission of the recipient of the message.

In co-pending application 09/626,577, a server transmits a message from a sender to a recipient. The message may pass through intermediate stations before it reaches the recipient. These intermediate stations, and the time for the transmission of

the message to the intermediate stations form a part of the record received at the intermediate station. The intermediate stations receiving this record in the transmission of the record from the recipient, and the times for the transmission of the record to the intermediate stations, are also included in the record received at the server. The server then transmits to the sender this record, the message, the digital signature of the message and the digital signature of the attachment(s) defined by the record(s) of the intermediate stations and the times of the transmissions to the intermediate stations.

When the sender wishes to authenticate the message and the file history of the transmission of the message between the sender and the recipient , the sender transmits this information to the server and the server processes this information to provide the authentication.

Generally the server is hired by the sender to act as the sender's agent in transmitting a message electronically to a recipient. Since the server acts as the sender's agent, the sender is interested in authenticating that the server has transmitted the message properly to the recipient and in authenticating the time of transmission of the message to the recipient. The system and method disclosed and claimed in co-pending application 09/626,577 provides these authentications.

Sometimes the recipient is interested in authenticating the message transmitted to the recipient and in authenticating the time of the transmission of the message to the recipient. For example, this is important when the sender is a United States or state court, and the recipient is an attorney involved in representing a client in a matter before the courts and the message relates to a document that the attorney has to file on a short time basis in the court. Under such circumstances, the attorney may wish to have the message authenticated promptly and the time of the transmission of the message to the attorney authenticated promptly. As will be appreciated, any system of method addressing this problem should be simple, prompt and reliable.

The mostly widely practiced methods for authenticating the authorship and content of electronic messages involve applications of Public Key Cryptography. In

such methods the sender of the message computes a digital digest or "hash" of the contents of the message and encrypts this information, together with other information identifying the sender, using the sender's private encryption key. The encrypted information is included as an attachment to the message. Upon receiving the message the recipient authenticates its authorship and content by applying the sender's public encryption key to decrypt the attachment and then compares the decrypted digital digest with a digital digest of the received message.

There are several shortcomings with this system:

- The system requires that the recipient possesses software capable of performing the necessary cryptography and possesses the requisite decryption keys. Some of the most commonly used mail clients, e.g., web based mail client, lack this capacity. The method is not universal among e-mail clients.

- When a message is "digitally signed" in this manner any change to the message however innocent will result in a failure to authenticate. For example, the changes typically introduced into a message by forwarding it from most e-mail clients will change the message's digest and will result in a failure to authenticate. PKI digital signatures are, in this sense, fragile.

- Finally, when a message fails to authenticate because it has changed, it is for all practical purposes, impossible for the recipient to know which portion of the message has changed or to reconstruct the original message. The method is not resilient.

In contrast the method described below is universal, non-fragile, and resilient.

BRIEF DESCRIPTION OF A PREFERRED EMBODIMENT OF THE INVENTION

A server provides a message from a sender to a recipient and an attachment including the sender's identity, the recipient's identity and address, and the time of transmission from the server to the recipient. Upon reception, the recipient transmits to the server the information sent to the recipient from the server. To authenticate the

message and the transmission to the recipient, the server produces digital signatures (hashed encryption) of the message and the attachment. The server then produces digital fingerprints of the digital signatures and digital fingerprints (hashed) of the message and the attachment. The server provides the authentication to the sender when the two (2) digital fingerprints relating to the message are identical and when the two (2) digital fingerprints relating to the attachment are identical. The authentication may also be provided to the recipient third parties associated with the recipient.

BRIEF DESCRIPTION OF THE DRAWINGS

Detailed description of the preferred embodiment of the invention will be made with reference to the accompanying drawings:

FIG. 1 is a system diagram of a first embodiment of an invention disclosed and claimed in co-pending application 09/626,577, in which embodiment outgoing messages are made of record by being transmitted by a special Mail Transport Agent (MTA);

FIGS. 2-2F constitute a representative flow diagram for making an outgoing e-mail of record according to the embodiment of FIG. 1;

FIG. 3 is a system diagram of a second embodiment of the invention disclosed and claimed in co-pending application 09/626,577, in which embodiment senders may direct a Mail Transport Agent to transmit selected messages through a separate Mail Transport Agent constructed to make the selected messages of record;

FIG. 4 is a system diagram of a third embodiment of the invention disclosed and claimed in co-pending application 09/626,577, in which embodiment carbon copies (cc's) of outgoing messages are sent to a special server to be made of record;

FIG. 5 is a system diagram of a fourth embodiment of the invention disclosed and claimed in co-pending application 09/626,577, in which embodiment users compose outgoing messages to be made of record at a designated website.

FIG. 6 is a system diagram of a fifth embodiment of the invention disclosed and claimed in co-pending application 09/626,577 in which embodiment users may send e-mails made of record and store receipts from within a Web Based Mail User Agent (MUA);

FIG. 7 is a flow diagram for validating an e-mail receipt made of record;

FIG. 8 is a system diagram of an embodiment of the invention disclosed and claimed in co-pending application 09/626,577 for making of record incoming messages;

FIG. 9 is a flow diagram in co-pending application 09/626,577 for making of record incoming messages;

FIG. 10 is a flow diagram in co-pending application 09/626,577 for validating received messages made of record;

FIG. 11 is a system diagram showing in co-pending application 09/626,577 an exemplary use of the system by an e-business to make of record and acknowledge incoming and outgoing communications; and

FIG. 12 is a block diagram showing a system and method operative in combination with the systems and methods shown in Figures 1-11 for authenticating to a recipient a message transmitted to the recipient and the time at which the message is transmitted to the recipient.

FIGS. 13 and 14 are flow charts, primarily in block form, of another system for, and another method of, authenticating to a recipient a message transmitted to the recipient, and attachments to the message, and the time at which the message is transmitted to the recipient.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

This description is not to be taken in a limiting sense, but is made merely for the purpose of illustrating the general principles of the invention. The section titles and overall organization of the present detailed description are for the purpose of convenience only and are not intended to limit the present invention. Accordingly, the invention will be described with respect to e-mail messaging systems that use the internet network architecture and infrastructure. It is to be understood that the particular message type and network architecture described herein is for illustration only; the invention also applies to other electronic message protocols and message types using other computer network architectures, including wired and wireless networks. For convenience of discussion, messages that are processed according to the invention disclosed and claimed in co-pending application 09/626,577 may be referred to herein as being "made of record" messages. In the discussion which follows, the term "RPost" will refer in general terms to a third party entity which creates and/or operates software and/or hardware implementing the present invention, and/or acts as a third party message verifier. The term is used for convenience of exemplary discussion only and is not to be understood as limiting the invention.

I. RPOST AS OUTGOING MAIL SERVER EMBODIMENT

FIG. 1 is a system diagram of a first embodiment of the present invention, wherein outgoing e-mails are made of record according to the invention disclosed and claimed in co-pending non-provisional application 09/626,577 . In this embodiment, the RPost server 14 serves as the primary outgoing Mail Transport Agent (MTA) for a message sender's Mail User Agent (MUA) 13. Although message recipient 18 is technically the addressee and is therefore merely the intended recipient or intended destination at this point in time, for simplicity of discussion this entity will be referred

to herein as the recipient, addressee, or destination. Note that a single message may have many different destinations and that each of these may be reached through a different MTA. The method of sending messages made of record may divided into three parts:

1) *Preprocessing*: Steps to be taken before a message is transmitted;
2) *Transmission*: The method of delivering messages to addressees;
3) *Post Processing*: Procedures for gathering information about messages after their delivery, the creation of receipts, and the validation of receipts.

I. 1. PREPROCESSING

On receiving a message for transmission, the RPost server 14 will create records in a database for each message that will be used to store such information as:

a) the time at which the message was received;

b) the names of the attachments of the message; and

c) the number of addressees of the message.

For each destination of the message, the database will record:

a) the name of the destination (if available);

b) the internet address of the destination;

c) the time at which the message was delivered to the destination's Mail Server; and

d) the *Delivery Status* of this destination.

Recipient Delivery Statuses used by the system will include:

UNSENT

This status indicates that the message has not been sent.

DELIVERED-AND-WAITING-FOR-DSN

This status indicates that the message has been delivered to an ESMTP compliant MTA that supports Delivery Status Notification (DSN) so that a success/failure notification can be expected.

DELIVERED

This status signifies that the copy of the message sent to this recipient has been successfully delivered to a server that does not support ESMTP DSN.

DELIVERED-TO- MAILBOX

This status signifies that a DSN message has been received which indicates that the copy of the message sent to this recipient was delivered to the mailbox of the recipient.

RELAYED

This status signifies that an MTA DSN has been received which indicates that the copy of the message sent to this recipient has been relayed onward to another server.

UNDELIVERABLE

This status indicates that after repeated attempts RPost has been unable to connect to an MTA to deliver the messages to this recipient.

FAILED

This status signifies that an MTA DSN has been received that indicates a failure to deliver a copy of the message to this recipient.

At this time the system will also perform hashing functions on the message's contents.

RPost server 14 employs a hash function and an encryption algorithm. The hash function may be one of any well-known hash functions, including MD2, MD5, the Secure Hashing Algorithm (SHA), or other hash functions which may be developed in the future. Hash algorithms and methods are described in Bruce Schneider, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc. (New York) 1993; Federal Information Processing Standard Publication 180-1 (FIPS PUB 180-1) Secure Hash Standard, National Institute of Standards and Technology; and U.S. Pat. No. 5,530,757 issued to Krawczyk, entitled "Distributed Fingerprints for Information Integrity Verification," which are hereby incorporated by reference for their teachings of hash functions, encryption, and methods and systems for implementing those functions. Other known or new methods of detecting whether the contents of the message have been altered may be used.

A good hash function H is one-way; that is, it is hard to invert where "hard to invert" means that given a hash value h, it is computationally infeasible to find some input x such that $H(x) = h$. Furthermore, the hash function should be at least weakly collision-free, which means that, given a message x, it is computationally infeasible to find some input y such that $H(x) = H(y)$. The consequence of this is that a would-be forger who knows the algorithm used and the resulting hash value or message digest will nevertheless not be able to create a counterfeit message that will hash to the same number. The hash value h returned by a hash function is generally referred to as a message digest. The message digest is sometimes referred to as a "digital fingerprint" of the message x. Currently, it is recommended that one-way hash functions produce outputs that are at least 128 bits long in order to ensure that the results are secure and not forgeable. As the current state of the art advances, the recommended length for secure hash functions may increase.

RPost server 14 computes a message digest for the message body, and a separate message digest for each of the attachments of the message and stores these in a manner in which they may be later included in a receipt for the message.

Before the message is altered in the ways that registration will require, a copy of the original message and its attachments are stored in a manner in which they can be later retrieved by the system.

The RPost server 14 may alter a message in several ways before transmission to the recipient's MTA.

Although such is not necessary to the practice of the invention, the message may be tagged to denote the fact that the message has been made of record, such as by inserting the words "Made of Record" or at the beginning of the "subject" line of the message, by appending a tag such as,

"This message has been made of record with RPost. Visit our web site at www.RPost.com for additional information."

at the end of the original message or other tagging. Additionally, the tag may contain instructions, World Wide Web addresses, or links that invite and allow the recipient to send a reply made of record to the message by linking to a Web Page from which messages made of record may be composed and sent.

Although tagging is optional, the delivered message will generally be referred to herein as the tagged message.

Internet protocols provide two forms of receipt for e-mail messages:

MTA NOTIFICATIONS

These are e-mails that are sent by a recipient's MTA notifying the nominal sender of the message that various events have occurred. MTAs that conform to the SMTP protocol will typically only send a notification in the event that the mailer cannot deliver a message to the mailbox of the addressee (as might happen if the

address is not valid or if the addressee's mailbox has exceeded its allotted storage quota).

With the introduction of the Extended SMTP standard it became possible for sending MTAs to request notices of success and failure in the delivery of messages. These Delivery Status Notifications (DSNs) are e-mails which are sent by a receiving MTA to the nominal sender of the message when certain events occur: e.g., the message has been successfully deposited into the mailbox of the recipient; the message cannot be delivered to the recipient's mailbox for some reason; the recipient's message has been relayed on to another server which does not give DSN receipts.

Note that only e-mail servers that support the Extended SMTP (ESMTP) protocol support this form of DSN and that support for this function is optional for ESMTP servers and depends on the configuration selected by the server's administrators.

Although DSN is a term that only came into use with the advent of ESMTP, we will, in what follows, use 'DSN' to refer to any MTA generated message relating to the status of a received message whether or not it is in conformity to the ESMTP protocol.

MUA NOTICES (READING NOTIFICATIONS)

These are e-mails that are sent to the (nominal) author of a message by the recipient's Mail User Agent (MUA) (e-mail program) when certain events occur: e.g., the message is opened for reading, or deleted from the system without being read. By internet convention (RFC 1891), no MUA program can be forced to generate such notifications. Whether an MUA will generate these receipts will depend upon the configuration chosen by its user.

The RPost server 14 will configure and transmit messages in a way that attempts to elicit both MTA DSNs and MUA notices from compliant MTAs and MUAs. In order to elicit a Reading Receipt from compliant MUAs, certain headers are preferably included in the header section of an e-mail message. Different MUAs respond to different headers; hence Server 14 will add several different headers to each

message requesting a read notification in a form recognized by various MUAs. These headers all take the form:

```
Header label: user name <user address>
```

For example:

```
Disposition-notification-to: john smith <jsmith@adomain.com>
read-notification-to: john smith  <jsmith@adomain.com>
```

where 'john smith' is the name of the user to whom an MUA notification is to be sent and '<jsmith@adomain.com>' is that user's internet address. Normally such headers would refer to the author of the message but in the case of the present method the notification should be returned to RPost so that the notification can be processed by RPost. To assure that this is so, Server 14 will insert headers that request that MUA receipts be sent to an address where they can be processed by the RPost server, for example: "readreceipt@RPost.com". This will direct any compliant recipient MUAs to send their notifications to an RPost address for processing.

The task of processing returned MUA notifications raises another problem that should be dealt with at this stage. There are no standards governing the format or content of MUA notifications. Often they will quote the subject of the original message and the time of the event (e.g. "opened for reading") that they are reporting. But even if this information is included in the notification, it is rarely sufficient to uniquely identify the message that prompts it or to identify the author of that message. When the system receives a MUA notification, it should identify the message that prompts it, so as to include the notification information in the receipt that RPost will generate for the sender. Alternatively, the system should reliably identify the sender of the message to which the MUA notification refers so that the notification information can be passed on to the sender in the form of an RPost Reading receipt (see below).

To accomplish the latter goal, the system can take advantage of the fact that internet addresses have two components: a name field and an address field, where the

address field is set off by corner quotes "<>". Most MUAs will include both fields in the destination address of their MUA notifications. In composing its requests for MUA receipts, the RPost system will include the server 14 read receipt-handling address as the address for the notification but will use the address of the original sender in the name field of the header. For example, where the original sender of the message is user John Smith with internet address jsmith@adomain.com, the RPost server 14 will include headers of the form:

```
Disposition-notification-to: jsmith@adomain.com <readreceipts@RPost.com>
```

This will typically result in the compliant MUA sending a notification to readreceipts@RPost.com addressed as:

```
jsmith@adomain.com <readreceipts@RPost.com>
```

On receipt of such a notification at the address "*readreceipts@RPost.com*", the server can, by parsing the addressee's field, determine that the notification concerns a message originally sent by *jsmith@adomain.com*, even if this could not be determined by any examination of the contents of the notification. With this information in hand, the server can then package the contents of the notification in a digitally signed RPost Reading receipt and send the receipt to the address jsmith@adomain.com

The RPost system will also endeavor to elicit and collect MTA DSN notices generated by recipient MTAs. Since such notifications are sent to the address listed in the "FROM:" field of the message header, the server 14 will alter each message header so that the message is received as "FROM:" an RPost address at which DSNs may be processed.

However the problem of processing DSNs raises another issue, which should be dealt with at this stage. DSNs do not have any standard content or format; often it is impossible to determine, merely by examining the contents of these e-mails, what message their contents are giving notification of. This problem was supposed to have

been addressed for DSNs generated in compliance with the ESMTP protocol by the use of DSN envelope ID numbers (see RFC 1869). According to the protocol, a transmitting MTA can include a reference number along with its request for a DSN. This number would be quoted in any returning DSN, allowing the sender to identify the subject message of the DSN. However, as a matter of fact, many MTAs that report themselves as supporting ESMTP DSN do not return a DSN envelope ID or any other information sufficient to reliably identify the subject message. Finally, even where a DSN does return information sufficient to identify the message it is giving notice of, it often will not contain sufficient information to identify the specific addressee of the message that has prompted the notification. Thus, a single message might be sent to two addressees at a domain; one might be successfully delivered to the addressee's mailbox; the other, not. The MTA for the domain may report these events in a DSN in ways that provide no way for the recipient of the DSN to determine which addressee was successfully delivered and which was not (as, for example, may happen if the DSN reports the recipient's addresses as their local alias names rather than by the addresses contained in the original message).

The present invention solves this problem in four steps:

1) A unique identification number is generated for each outgoing message (e.g. based upon a time stamp). This number is stored in a database.

2) The recipients of each message are enumerated and the identifying numbers are stored in a database.

3) The message is sent separately to each intended recipient's MTA. (Even when two recipients have a common domain name and MTA, the server 14 will transmit the message to that MTA in two separate SMTP telnet sessions.)

4) When the server 14 transmits the message to a recipient's MTA it augments the message's "FROM" field to show the message as having been sent from an address which incorporates the message's unique ID and the identifying number of the sender. The address also contains a substring (e.g. "rcpt") that enables the server to identify return messages as DSNs.

Thus, a single message denominated "mmyyddss" by the server 14, from the sender named John Smith, might be sent to its first intended recipient (denominated "a" by the system) with a header reading:

```
From: John Smith <rcptmmddyyssa@RPost.com>
```

The same message would be sent to the second recipient with a header reading:

```
From: John Smith <rcptmmddyyssb@RPost.com>
```

Many e-mail MUAs will only display the name of the sender of a message and thus the special address will be unseen by most recipients.

The upshot of this form of addressing is that when the recipient MTAs issue DSNs (whether ESMTP compliant or not) they will address those DSNs to different RPost addressees. On receiving these DSNs, the server 14 can identify them as DSN messages by their "RCPT" prefix and, by parsing the addressees, can determine which message and which recipient is the subject of the DSN.

The server 14 will alter the 'FROM' field of each message to refer to a recipient of the message each time it attempts to transmit the message to that recipient's MTA.

To insure that recipient replies to transmitted messages are directed properly the server 14 will add an explicit "reply-to:" message header into the message listing the original sender's name and internet address. In the case of the present example this would be:

```
Reply-to: john smith <jsmith@adomain.com>
```

This will lead recipient MUAs to address replies to a received message to the actual sender's address, rather than the constructed RPost address.

I. 2. TRANSMISSION

As noted above, it is part of the method that the RPost server 14 transmits a separate copy of an outgoing message to each addressee of that message. Moreover RPost will attempt to make each such delivery through a direct SMTP connection with a mail exchanger (MX) of record for each destination.

Note: Each valid internet e-mail address includes an internet domain name or IP address. Each domain name/address has associated with it an e-mail server(s) authorized to receive mail for addresses in that domain. It will be noted that some domains have more than one server. The Domain Name Server responsible for each domain broadcasts the identity of its mail servers across the internet. This information is publicly available and is managed and transmitted in ways that conform to rules and conventions which govern internet e-mail and Domain Name service.

Before transmitting a copy of a message to any destination, the RPost server 14 will perform an internet Name Server Lookup to identify an MTA associated with the destination's domain. Having identified the MTA responsible for receiving mail on behalf of a destination address, the system will attempt to open a telnet connection with the destination's local MTA.

It is common practice for internet e-mails to be relayed from MTA to MTA until they reach their final destination. The primary purpose for providing a direct connection between the RPost server 14 and the destination's MTA is so that the RPost server can record delivery of the message, (this record taking the form of an SMTP dialogue) with the e-mail server which has proprietary responsibility for receiving e-mail for the recipient domain name.

The existence of this record provides helpful evidence that the message was delivered, in much the same way that a registered mail receipt provides evidence of

delivery. USPS Registered mail is treated as verifiably delivered if it can be proved to have been delivered to the addressee's authorized agent (e.g. a secretary, or mail room clerk). In the event of any legal challenge to the evidentiary merit of an RPost delivery receipt, it will be recognized that in selecting an internet e-mail service provider, the recipient has authorized that provider to collect electronic messages on his or her behalf. In turn, that service provider has acknowledged its status as the authorized agent for e-mail recipients of that domain name by broadcasting the address of its MTAs as the receptive e-mail servers for this domain.

Accordingly, having delivered messages directly to the mail server responsible for receiving the recipient's e-mail, RPost will have delivered the message to an agent the recipient has legally authorized to receive his mail. By recording the delivery transaction (that transaction taking the form of an SMTP dialogue) RPost can claim to have proof of delivery to the recipient's authorized agent.

Note that while the method herein described attempts to collect other forms of proof of delivery to each destination, whether or not these attempts succeed will depend upon factors that will not be in the control of RPost, (e.g. the form of SMTP support deployed on the recipient's mail server). On the other hand, every successful delivery direct to a recipient's mail server will always generate an SMTP record. Recording this record allows RPost to provide proof of delivery to any valid internet destination that complies with the minimum protocols (SMTP) for internet mail. This represents an important advantage of the current method over other methods that might attempt to prove delivery by reliance on ESMTP DSN.

Having identified the MTA for a destination of a message, the RPost server 14 will attempt to open an ESMTP connection with the destination MTA by issuing an "EHLO" handshake in compliance with RFC 1869. If SERVER 16 supports ESMTP, it will respond by listing which ESMTP services it supports.

If SERVER 16 supports ESMTP, the RPost server 14 will first determine if SERVER 16 supports the ESMTP Service "VERIFY". The Verify service allows a

calling SMTP server to determine, among other things, if an address in an MTA's domain is genuine. If the RPost server 14 determines by these means that the address it is attempting to deliver its message to is not valid, it will terminate the connection, cease attempting to deliver a message to this addressee, and record, in its database, the status of this message destination as UNDELIVERABLE.

Whatever its result, the RPost server 14 will record the ESMTP VERIFY dialogue in a file and store it so that it may be later attached to or included in the Delivery Receipt for this message. It should be noted that, out of concern for security, few ESMTP servers support the VERIFY function.

If System 16 does not support the VERIFY method, then the RPost server 14 will nevertheless attempt to deliver the message to System 16. Typically an MTA will accept messages for any address nominally in its domain and will later send a DSN if the address is invalid.

The RPost server 14 will then attempt to determine if the destination server supports the ESMTP service DSN. If it does, RPost will transmit the message with a request that SERVER 16 notify the sender of the message with an ESMTP DSN if the delivery to the addressee succeeds or fails. After the successful transmission of the message to this destination the system will record the Delivery Status of this destination as DELIVERED-WAITING-FOR-DSN.

If Server 16 replies to the "EHLO" handshake in a way that indicates that it does not support ESMTP, the RPost server 14 will issue a "HELO" message to initiate an SMTP connection. If this connection is achieved, the RPost server 14 will transmit the message in compliance with the SMTP protocol and will record the Delivery Status of the destination as DELIVERED.

Whether the connection is SMTP or ESMTP, the RPost server 14 will record the entire protocol dialogue between the two servers. Typically this dialogue will include protocol messages in which, among other things, the destination server identifies itself, grants permission to upload a message for a named recipient, and

acknowledges that the message was received. RPost will save the record of this transaction in such way that it may be later retrieved and included in or attached to the RPost Delivery Receipt for this message.

For various reasons RPost may not be able to achieve an SMTP connection with an MTA of a recipient or it may achieve such a connection but be denied permission to transmit the message by the recipient. In that case, if the internet DNS lookup reveals that the destination address is served by multiple MTAs, the RPost server 14 will attempt to deliver its message to each of these in turn. RPost will continue to attempt to deliver to an appropriate MTA as often as system resources permit. If, after a length of time, RPost cannot deliver the message to an address, it will mark the status of this recipient of this message as "UNDELIVERABLE" and stop attempting to send this message to this destination address.

When the RPost server 14 succeeds in transmitting a message to a destination Server that explicitly supports ESMTP DSN, RPost will record the status of this recipient for this message as "DELIVERED-AND-WAITING-FOR-DSN".

When the RPost server 14 succeeds in transmitting a message to the destination Server via a connection that does not explicitly support ESMTP DSN, RPost will record the status of this recipient for this message as "DELIVERED."

I. 3. POSTPROCESSING

DSN Processing

MTA DSNs will be returned to the RPost server 14 addressed to fictitious addresses in its proprietary domain (e.g. "RPost.com"), these addresses having been constructed as described above. The RPost server 14 will scan all inbound mail addressed to the domain and detect DSN messages by their identifying substring (e.g. "rcpt"). By parsing these addresses in the manner described above, the system can identify the message and the recipient that has prompted the DSN notification.

There is no standard format for DSN messages; neither is there any standard lexicon in which they report their results. To evaluate a received DSN the system should look in the subject line and the body of DSN messages for words and phrases that express the DSN's meaning. For example, such phrases as "successful delivery" or "delivered to mailbox" or "was delivered" normally signal that the message the DSN concerns was deposited to the mailbox of the destination. When it detects such phrases the System will change the Delivery Status of this destination of the message to "DELIVERED TO MAILBOX".

Phrases such as "could not be delivered", "fatal error", "failure" and "unsuccessful" typically signal a DSN that reports a failure by the MTA to deliver the message to the destination. When it detects phrases such as these in the DSN, the system will change the record of the recipient's Delivery Status to "FAILED".

Though the system always delivers mail to a proprietary MTA for the destination's domain, these MTAs will sometimes relay the message to a different server (as may be the case, for example, if the receiving MTA sends mail behind a firewall). In this case the DSN will contain such phrases as "relayed" or "relayed onward". In such cases the system will change the recipient's Delivery Status to "RELAYED".

Having evaluated the DSN and updated the recipient's Delivery Status accordingly, the system will save the DSN and any attachments it may contain in such a way that this message(s) may be included in and/or attached to an RPost Delivery Receipt.

Message Management

From time to time the system will scan each sent message and examine the status of each destination of that message in order to determine if the system has completed processing of that destination's delivery. The criteria for completion depend upon the destination's Delivery Status:

DELIVERED: This status indicates that a copy of the message for this recipient has been delivered to an MTA that does not support ESMTP DSN. Such an MTA may nevertheless send a form of Delivery Status Notification in the event that the message could not be delivered to the Mailbox of the addressee (as might happen, for example, if the destination address does not correspond to a valid account within the domain). Accordingly, the system will not treat the delivery for such a recipient as completed until a period of time has elapsed since the delivery to the recipient MTA. This time period--typically two to twenty-four hours--represents an estimate of the maximum time required for a majority of servers to return a notification of a failure to deliver and it may be adjusted if the specific destination domain is remote or known to be prompt or tardy in producing such notifications.

RELAYED: This status signifies that a DSN has been received that indicates that the recipient MTA has forwarded the message to another MTA that does not support ESMTP DSN. In this case it is nevertheless possible that the MTA to which the message has been delivered will send a notification of failure to deliver in due course. Accordingly recipients with this status are treated as complete under the same conditions as recipients with the status DELIVERED.

DELIVERED-AND-WAITING-FOR-DSN: This status indicates that the recipient's MTA supports ESMTP DSN and that a DSN has been solicited but not yet received. It may sometimes happen that although an MTA identifies itself as supporting this service it will nevertheless not provide DSNs even in the event of successful delivery. Accordingly, the system will regard deliveries to a destination with this status as completed even if no DSN is received after an interval of time. This interval--typically six to twenty-four hours--represents an estimate of the maximum time typically required for a compliant MTA to return a DSN.

DELIVERED-TO-MAILBOX: This status indicates that a DSN indicating successful delivery has been received for this recipient and hence the delivery of the message to this destination is completed.

FAILED, UNDELIVERABLE: Deliveries to recipients with this status are always treated as complete.

When the system finds that delivery to all recipients of a message has been completed the system will construct a Delivery Receipt for the message.

Creation of Delivery Receipts

Delivery receipts are e-mails sent to the original sender of the made-of-record message. The receipt 20 may contain:

1. an identifier for administrative purposes. This identifier may be or may include reference to the sender's ID and/or the value of the internet Message-ID of the sender's message as received by the system;
2. the date and time at which the receipt was generated;
3. the quoted body of the original message together with the e-mail addresses of its intended recipients;
4. the date and time at which the RPost server received the message;
5. a table for each destination listing:
   (i) the time at which the recipient's MTA received the message and/or the time at which the system received a DSN report from the recipient's MTA;

   (ii) a Delivery Status of the message for that destination. The Delivery Status quoted in a Delivery Receipt is based upon the system's internal record of the destination's Delivery Status. They may be transcribed as follows:

- Deliveries to destinations whose status is FAILED or UNDELIVERABLE will be recorded in the receipt as "failed".

Deliveries to destinations whose status is DELIVERED or DELIVERED-AND-WAITING-FOR DSN will be recorded in the receipt as "delivered to mail server".

- Deliveries to recipients whose status is DELIVERED-TO-MAILBOX will be recorded in the receipt as "delivered to mail box".

The purpose of these reports is to accurately apprise the reader of the form of verification of delivery the system has been able to achieve.

6. a list of the original attachments of the e-mail together with the separate message digests of those attachments;
7. copies of the attachments to the original message, each original attachment being attached as an attachment to the receipt;
8. transcripts, summaries, or abstractions of the transcripts of all of the SMTP dialogs involved in the delivery of the message to each destination;
9. quotations from the bodies and the attachments of all received DSN reports including whatever details of delivery or disposition of the message that they might reveal; and
10. any files that were returned to the system as attachments to DSN reports.

All of these separate elements of the receipt may have their own message digests or digital signatures included within the receipt. Additionally, the receipt may include a single overall encrypted message digest or digital signature computed and appended as part of the receipt, thus providing a single message authentication code which could be used to authenticate all of the information contained within the receipt. Since the receipt itself and SMTP dialogs and DSN reports within the receipt contain time-stamps, the receipt includes a non-forgeable record of the message recipient(s), the message content, and the time(s) and route(s) of delivery.

MUA Notification Processing

MUA Notifications could be collected and incorporated within RPost Delivery receipts in the same manner as MTA DSNs. However, MTA notifications are typically issued by receiving MTAs within a few hours of delivery whereas MUA Notifications will not be generated, if ever, until the recipient opens his MUA e-mail client and takes some action with respect to the received mail. For this reason, in this embodiment of the invention MUA notifications are collected separately from MTA notifications and reported in "RPost Reading Receipts" separate from RPost Delivery Receipts.

MUA notifications elicited by message headers constructed in the manner described above will be returned to a common RPost address (e.g. "readreceipts@RPost.com") and each notification will contain-- in the name field of its address-- the address of the original sender of this message. Because this is the only information required to generate an RPost reading receipt in the manner described below, the system can deal with MUA notices whenever these notices may arrive and without any need to have stored any information about the original message in its data banks.

MUA notices may report, among other things, that a message has been read by a recipient, that a message has been displayed on the recipient's terminal (whether or not read), that a message has been deleted without having been opened. There is no protocol-governed standard for the content or format of MUA messages. The system could be configured so as to examine the text of MUAs to interpret their reports in the same fashion as the system uses for MTA DSNs. However, in the current embodiment of the invention, MUAs are not evaluated or interpreted by the RPost server 14 but are, instead, passed on to the sender for his own evaluation in a form that can be authenticated by RPost. To accomplish this the system will create an e-mail message styled as an "RPost Reading Notice" which may include, among other items:

1. subject line of the received MUA notice;

2. the body of the received MUA notice quoted as the body of the Reading Notice;
3. the received MUA notice included as an attachment;
4. any attachment(s) to the received MUA notice included as an attachment(s).
5. message digests of the received MUA notice and of any attachment(s) to that notice;
6. a date and time stamp;
7. an encrypted hash of at least items 5 and 6 providing an authenticatible date stamped digital signature for the document and all of its contents.

Receipt Disposition

In the case of the current embodiment of the invention, both RPost delivery receipts and Reading Notices are sent to the original sender of the made-of-record message. Since these receipts are digitally signed with an encrypted hash (i.e., a digital signature), RPost can authenticate the information contained in these messages any time they are presented to RPost for this purpose, in the manner described below. This means that once it has transmitted a copy of the receipt to its sender (with instructions to the sender to retain the receipt for his records), RPost has no further need to retain any data concerning the message or its delivery and may expunge all such records from its system. Thus, RPost need not keep any copy of the original message or the receipt. This economy of archival memory gives the present invention an advantage over various prior art message authentication systems that required large amounts of data storage at the service provider side.

In this case the burden of retaining receipt data falls on the original sender of the message. Alternatively or additionally, third party verifier RPost may, perhaps for an additional fee, store a permanent copy of the receipt or of some or all receipt data. The receipt or part(s) thereof may be kept on any suitable archival storage devices

including magnetic tape, CD ROM, or other storage device types. Additionally or alternatively, RPost may return receipts or parts thereof to a storage system devoted to this purpose within the control of the sender or the sender's organization.

As described above, RPost receipt information includes all of the data from the original sender's message and its attachments. There are circumstances in which users of the system might not wish to undertake the burden of retaining receipts in their records (e.g., out of fear of accidental data loss) but might also not wish to have the contents of their message in the hands of the RPost third party. Accordingly RPost might discard the contents of messages but store in its database only such information (e.g. sender, date of composition, message digests, destinations and Delivery Statuses) as might be provided by RPost to authenticate and verify the delivery of a message when presented with a copy of the message retained by the sender.

Verification

In the event that the originator of a message requires evidence at a later date that an e-mail was sent, delivered, and/or read, the originator presents the receipt(s) for the message to the operators of the system.

For example, in order to prove that a particular message was sent from sender 10 to recipient 18, sender 10 sends to RPost a copy of receipt 20 with a request to verify the information contained within the receipt. This could be done by sending the receipt to a predefined mailbox at RPost, e.g., verify@RPost.com. RPost then determines whether or not the receipt is a valid receipt. A receipt is a valid receipt if the digital signature matches the remainder of the receipt, and the message digests match the corresponding respective portions of the original message. Specifically, RPost performs the hash function on the various portions of the message including the message body, the attachments, and the overall message including the SMTP dialog and DSN reports, to produce one or more message digests corresponding to the purported message copy. RPost compares the message digests in the purported copy, including the overall message digest, with the message digests which RPost has

computed from the purported message copy. The overall message digest can be compared by either decrypting the overall message digest received as the digital signature in the purported receipt, or by encrypting the overall message digest which was calculated from the purported message copy. If the message digests including the digital signature match, then the receipt is an authentic RPost-generated receipt. Assuming that a good hash function was used and that the keys used in the cryptographic hash function and the digital signature encryption algorithm have not been divulged to others, it is virtually impossible that the receipt has been "forged" by the person presenting the receipt. That is, the receipt must have been a receipt that was generated by RPost, and therefore the message contained in the receipt, the to/from information, the date and time of delivery, the fact of successful delivery, the route by which the message traveled, and any DSN information contained within the receipt, must be a true copy of that information and is accurate. RPost can then provide authentication, verification, and confirmation of the information contained within the receipt. This confirmation can take the form of an e-mail confirmation, affidavit testimony from RPost employees familiar with the methods used by RPost, live sworn testimony in depositions and in court, and other forms of testimony. RPost can charge sender 10, recipient 18, or any other entity, fees for the various respective confirmation services. RPost can also provide testimony or other confirmation with regard to the non-authenticity of a purported receipt. Testimony may be provided in accordance with Federal Rules of Evidence 901(9), 901(10), 803(6), 803(7), 1001-1004, 1006, 702-706, corresponding state rules of evidence, and other applicable rules.

In sum, the system provides reliable evidence based on the testimony of a third party that a particular message having a particular content was sent, when it was sent, who sent it, who received it, when it was opened for reading, and when it was deleted. This evidence can be presented any time a dispute arises regarding the content and delivery of messages, as for example in contract formation, the timing of stock buy or sell orders, and many other applications. The operators of the system can attest to the

accuracy of the information contained in the receipt itself without the need for the operators to preserve any record or copy of the information contained in the receipt.

A significant advantage of the system is that it can be used by existing MUAs without any change thereto. Because all the computation, encryption, ESMTP interrogation and dialog, DSN report collection, and receipt compilation, are performed by the third party RPost server 14, none of these functions need to be implemented within any of the user's equipment. Thus, users can take advantage of the system quickly and easily.

In the embodiment of the invention described above, the RPost server 14 makes of record the delivery of all messages passing through it. Alternatively, an RPost server 14 might make of record only those messages having certain destinations (e.g. external to an organization) or from certain senders (e.g. a customer relations group). Alternatively or additionally, the RPost server 14 might make of record only those messages that had distinguishing characters or strings in the subject or body of the message. For example, the server might make of record only messages that the sender had included "(Make of Record)" or "(MR)" in the subject of the message. All other messages might be delivered by the RPost server 14 or some other server function as an ordinary internet MTA.

In this embodiment, RPost can raise revenue in a variety of ways. For instance: RPost can charge message sender 10 or her organization a fee on a per-message basis, on a per-kilobyte basis, on a flat fee periodic basis such as monthly, or on a combination of the above. RPost can also charge fees for authenticating and verifying a receipt, with a schedule of charges depending on whether the verification sought is a simple return e-mail, a written affidavit or declaration, sworn fact testimony in deposition or in court, or sworn expert testimony in deposition or in court. If the users opt to have RPost retain copies of the receipts, RPost can charge per item and/or per-kilobyte per month storage fees.

II. FLOW DIAGRAM FOR MAKING OF RECORD AN OUTGOING MESSAGE

FIGS. 2A-2G constitute a flow chart showing an exemplary operation of the first embodiment of the system. Modifying this flow chart to apply to other embodiments is within the skill of one familiar with software and e-mail protocols.

FIG 3A, Pre-processing, illustrates the steps taken with a message before it will be transmitted by the Making of Record Server (the System).

To make of record an e-mail message, in step 201 an originator/sender/user creates an e-mail message using any internet Mail User Agent (MUA). Possible MUAs include: (1) client side e-mail programs; (2) server based e-mail programs; (3) web based e-mail services; and (4) HTML forms submitted through web pages. The message may contain attached files as described in the Requests for Comments (RFCs) 822, 2046, and 2047, which are hereby incorporated by reference. RFCs are a series of notes regarding the internet that discuss many aspects of computer communication, focusing on networking protocols, procedures, programs, and concepts.

In this embodiment, the system functions as the sender's outgoing mail server and hence the sender's message will be directly transferred to the RPost server by the sender's MUA (step 202).

In step 203, the system creates a copy of the original message to be stored for later processing.

In step 204, the system creates a record in a database which may include such information as: the time at which the message was received by the server, the names and size(s) of the file attachment(s) of the message, the name (if known) of each destination of the message; the internet address of each destination; the time at which the message was delivered to the destination's MTA (initially this value is null) and a unit which records the **Delivery Status** of each destination.

In step 205, the Delivery Status of each destination is set to "UNSENT".

In step 206, the system generates and stores a message digest or digital signature generated from the message body.

In step 207, the system generates and stores a hash or message digest for each attachment included in the message.

In step 208, the system may create a modified copy of the original message. In this second copy (step 209), the original subject line of the message may be amended to indicate that this copy is made of record (e.g. by pre-pending "Made of Record").

In step 210, a notice that the message is made of record by the system together with links to the system's Word Wide Web site may be appended to the body of the message.

In step 211, the e-mail headers may be added requesting reading notification in a variety of header formats recognized by various MUAs. The requests for notification direct the return notification to an address associated with the system: for example, "readreceipt@RPost.com". These headers will also include the address of the original sender of the message in the name field of the address to which the MUA notification should be sent.

Preprocessing having been completed, the system will now transmit a copy of the message to each of its destinations as illustrated in FIG 2B.

Fig 2B illustrates the steps provided to transmit a message made of record. As step 220 indicates, the process provides a separate transmission for each recipient of the message.

In step 221, the system changes the header field of its working copy of the message to show the message as being "FROM:" a sender whose name is the original sender of the message but whose address is an "RPost.com" address constructed from:

a) a string used to identify returning MTA notifications (e.g. "RCPT");

b) a string which uniquely identifies the message being sent;

c) a tag which uniquely identifies the destination this copy of the message is being sent to.

In step 222, using the domain name of the destination currently being sent to, the system does a Domain Name Server Mail exchange lookup to find the address of the MTA(s) responsible for collecting mail for addresses in this domain.

In step 223, the system attempts to make a direct telnet connection to the MTA of the destination. If the connection fails, the system will try to make the connection again. Provided that the system has not exceeded a maximum number of retries (227) for this destination, the system will try to remake the connection perhaps using another MX server for the destination's domain (228).

If, after a maximum number of retries, the system cannot connect to an MTA for this destination, the system will, as in step 226, record this destination's Delivery Status as "UNDELIVERABLE" and cease attempting to deliver this message to this destination.

On connecting to the destination's MTA, the system will begin making a record of its (E)SMTP dialog with the MTA (225).

In step 229, the system attempts to initiate an Extended SMTP (ESMTP) exchange with the destination MTA by issuing an "EHLO" greeting.

If the destination's MTS supports ESMTP, the system will then (230) determine if the destination MTA supports the SMTP function VERIFY. If the MTA supports VERIFY, the system will attempt to determine if the destination address is a valid address within the domain (231).

If the address is not valid, then, as in step 232, the system will record the Delivery Status of this destination as "FAILURE" and will cease attempting to deliver this message to this destination.

If the address is valid or if the ESMTP server does not support VERIFY, the system will then (233) determine if the receiving MTA supports the ESMTP service DSN (Delivery Status Notification).

If the MTA does support ESMTP DSN, the system will transmit the message with ESMTP requests to notify the nominal sender of the message of delivery success

or failure (234). Having transmitted the message, the system will record the Delivery Status of this destination as "DELIVERED-AND-WAITING-FOR-DSN" (235).

If the receiving MTA does not support Extended SMTP, the system will transmit the message using SMTP (236) and record the destination's status as "DELIVERED" (237).

Having delivered the message, the system will then store the (E)SMTP dialog, recording the delivery in a manner in which it can later be recovered (238) and attempt to send the message to another destination.

Having transmitted a message to its destination(s), the system must perform several functions in order to gather information about the message's disposition. Fig. 2C illustrates the process by which the system processes MTA Notifications returned by recipient MTAs.

Because of the format used in the headers of sent messages illustrated in Fig 2B step 221, MTA message notifications will be delivered to a fictional local address at the server. The system will be able to detect these notifications by a string (e.g. "rcpt") embedded in their addresses (241). By parsing the address, as illustrated in 242, the system can determine which message to which destination prompted the received notification.

In step 243, the system scans the subject line and the body of received MTAs for phrases that indicate whether the MTA is reporting a successful delivery, a failed delivery, or that the message has been relayed to another server.

In the event that the process at step 243 reveals that the notification is reporting a successful delivery, the system will, as illustrated in step 245, change the Delivery Status of the relevant destination of the relevant message to "DELIVERED-TO-MAILBOX".

If the system determines that the MTA notice is reporting a delivery failure, the system will (247) change the Delivery Status of the relevant destination of the relevant message to "FAILURE".

In the event that the system determines that the MTA notification indicates that the message was relayed to another server, the system will, as illustrated in step 249, change the Delivery Status of the relevant destination of the relevant message to "RELAYED".

Having processed the MTA Notification, the system will save this message and all of its attachments in such manner that they may be later recalled and used in construction of a receipt for this destination (250).

From time to time, as illustrated in Fig. 2D, the system will examine the status of each message to determine if the system has recovered all of the MTA notifications it is likely to receive for each destination of message and may hence proceed to construct a receipt for the message.

The system will examine the Delivery Status of each destination of the message.

If any destination has the Delivery Status "UNSENT", then the processing of the message is not complete. (252).

If the Delivery Status of a destination is "DELIVERED-AND-WAITING-FOR-DSN", then the system will not regard the processing for this destination as complete unless, as is illustrated in step 254, the time since delivery of the message has exceeded the system's waiting period (e.g. 24 hrs.).

If the Delivery Status of a destination is "DELIVERED", (257) then the system will regard the processing of this destination as complete provided (258) that a period of time has elapsed which the operators of the system treat as sufficient to have received notice of delivery failure from the destination's MTA. (e.g. 2 hours).

Any other destination Delivery Status (e.g. "FAILED", "UNDELIVER-ABLE", "DELIVERED TO MAILBOX") is treated as having completed processing.

If processing of any of a message's destinations is not complete the system takes no action but moves to consider other messages in the system (step 255).

However, as illustrated in step 259, if processing of every destination of the message is complete, the system will generate a Delivery Receipt for the message.

As illustrated by way of example in FIG. 2E, the receipt may include:

An identifier for administrative purposes as in block 271. This identifier may be, or may include, reference to the sender's ID and/or the value of the internet Message-ID of the sender's message as received by the system.

As in block 272, the quoted body of the original message 12 together with the e-mail addresses of its intended recipients may also be included.

As in block 273, a table for each recipient listing may include:

a) the time at which the recipient's MTA received the message and/or the time at which the system received DSN from the recipient's MTA;

b) the Delivery Status report of the message for that destination, i.e., "Delivered to Mail Server", "Delivered to Mail Box", "Relayed", "Delivery Failure", or "Undeliverable".

As in block 274, a list of the original attachments of the e-mail together with their separate hash values or message digests.

As in block 275, transcripts or abstractions of the transcripts of all of the SMTP dialogs involved in the delivery of the message to each destination.

As in block 276, quotations from the bodies and the attachments of all received DSNs including whatever details of delivery or disposition of the message that they might reveal.

As in block 277, the system may attach to the receipt copies of all of the attachments of the original message, and, as in block 278, the system may additionally attach files returned to the system as attachments to DSNs.

In step 279, having generated the text of the receipt so far, the system then generates a first hash for the e-mail message and a second hash(es) for any attachments to the body of the receipt and calculates a digital signature for each of the hash(es) using an encryption key known only to the operators of the system. Encryption can employ, for example, the Data Encryption Standard described in Federal Information Processing Standard Publication 4-2 (FIPS PUB 46-2), the Data Encryption Standard, National Institute of Standards and Technology, which is hereby incorporated by reference. Alternatively, other known or new methods of encrypting the hash value may be used.

In step 280, the encrypted hash is then appended to the end of the message as the "document digital signature".

In step 281, the receipt 20, now being complete, may be sent by e-mail to the sender with the advice that it be kept for the sender's records. In step 282, the system may now delete all copies of the original message, attachments, and DSNs. Alternatively, rather than sending the receipt to the sender, the system may store the receipt, or both the sender and system can store the receipt.

Because MUA notifications are returned only at the option of the recipient and only when the recipient takes some action with respect to the received message, embodiments of the system may choose to treat these return messages differently than MTA notifications.

FIG. 2F illustrates how these MUA notifications may be treated by the system. MUA notifications are solicited by the system by including various headers in outgoing messages in the manner of Fig 2A, step 211. These headers direct compliant

MUAs to send notifications to a system address (e.g. "readreceipt@RPost.com") set aside for this purpose. The headers also use, in the "name" field of this return address, the e-mail address of the original sender of the message. Accordingly, in step 286, when MUA notifications are returned to readreceipt@RPost.com the system can, by examining the address of the notification, determine the address to which a reading notification should be sent.

Upon the arrival of a read receipt from a destination's MUA, the system, in step 287, generates a reading receipt that contains the subject of the received MUA notification as its subject and incorporates, in its message body, the body of the received MUA Notification.

In step 288, the system attaches to the receipt any files that may accompany the MUA's receipt (typically these may include details of delivery or disposition and identifying references to the original e-mail.)

In step 289, the system generates a hash for any files attached to the receipt and records this hash in the body of the receipt.

In step 290, the system generates a hash for the body of the receipt and its attachments, encrypts this hash, and appends the result to the message as a "document digital signature".

In step 291, the system sends the resulting receipt to the sender of the message. In step 292, having sent this receipt, the system may delete all internal records of the transaction.

III. RPOST AS SECONDARY MAIL SERVER EMBODIMENT

FIG. 3 is a system diagram of a second embodiment of the present invention wherein the RPost server 14 does not serve as the user's primary MTA but rather works in collaboration with another MTA. In this embodiment, the sender may elect to make of record a particular outgoing message by including some form of flag in an

outgoing message, message subject, or message addresses. For example, if and only if a sender includes the symbol "(Made of Record)" or "(MR)" in the subject of the message the sender's MTA will direct the message to be transmitted through the RPost server 14 to generate a receipt.

In this embodiment the operators of RPost receive revenues from the operator of the sender's MTA per message and/or per kilobyte transmitted.

IV. CC TO RPOST EMBODIMENT

FIG. 4 is a system diagram of a third embodiment in which a carbon copy ("cc") is sent to the RPost server 14. In this embodiment, the user or message sender 10 can use a standard MUA and standard MTA without modification. Message sender 10 composes the e-mail having a message body and any number of attachments, and addresses it to message recipient 18, along with any carbon copies (cc's) and blind carbon copies (bcc's) as desired. Additionally, message sender 10 addresses a cc to RPost. RPost server 14 tags the message as before, and sends the tagged message including attachments to the recipient's MTA 16 and any designated cc's. On receipt of such a copy RPost server 14 may send an e-mail acknowledging receipt of the copy.

Recipient 18 and other destinations of the message will now receive two versions of the same message: a first version of the message received directly from sender 10, and a second and tagged version which was forwarded from RPost. Once RPost receives confirmation from recipient MTA 16 that the tagged version of the message was successfully received by recipient MTA 16, RPost server 14 composes message receipt 20 as before and sends the receipt to sender 10 for his records.

Revenue can be generated by establishing accounts for message originating domains or individual message senders, and charging the users' accounts per message, per kilobyte, per month, or a combination of these. Revenue can also be generated for

the placement of advertisements on receipts and from authentication and verification services as previously described.

V. WEBSITE EMBODIMENT

FIG. 5 is a system diagram of a fourth embodiment. In this embodiment, RPost server 14 is associated with a website at which a user composes messages. Message sender 10 visits the RPost Website and composes his message at the website by entering the desired "to", "cc", "bcc", "Subject", and message text information. Attachments can be added by using features available on standard browsers and web servers. In this embodiment, the sender additionally provides an address to which the made-of-record receipt may be sent. RPost server 14 sends the receipt to sender 10 through sender's MTA.

Revenue can be generated by establishing accounts for message originating domains or individual message senders, and charging the users' accounts per message, per kilobyte, per month, or a combination of these. Revenue can also be generated for the placement of advertisements on receipts and from authentication and verification services as previously described.

VI. WEB BASED MUA EMBODIMENT

FIG. 6 is a system diagram of a fifth embodiment. In this embodiment, the RPost server 14 is associated with a web based Mail User Agent. In addition to allowing users to compose mail through a web browser, such a MUA provides subscribers with browser viewable mailboxes that display messages stored on the web server site. Subscribers to such a service gain access to mail accounts with user names and passwords. In this embodiment, message sender 10 visits the RPost website, accesses a web based e-mail account by entering a user name and password, and composes his message which is transported for delivery to RPost server 14. Receipts

generated by the RPost server 14 are returned to a web based mailbox associated with the subscriber's account.

In addition to the revenue sources available in other embodiments, in this embodiment the operators can charge storage fees for receipts held in the web based mailbox.

In all of these embodiments, the receipt may serve as evidence that:

(1) the originator sent an e-mail message;

(2) the message was sent at a certain time;

(3) the e-mail was addressed to certain recipient(s);

(4) the e-mail was delivered to the e-mail mailbox of each of its intended recipient(s);

(5) the e-mail was delivered at a certain time;

(6) the e-mail was delivered by a certain network route; and

(7) the e-mail message and its attachments had the specific content recorded in the receipt.

Furthermore, the system under certain circumstances generates a separate receipt, which may be used as evidence that:

(1) the e-mail was inspected through the recipient's Mail User Agent (MUA); and

(2) the recipient took certain actions in response to the message, e.g., read or deleted the e-mail, at a particular time.

As with the other embodiments, this embodiment produces documented evidence which may be attested to and verified by the disinterested third party

operators of the system concerning the delivery and integrity of an electronic message. In other words, the system can be thought of as transforming the e-mail to a made-of-record e-mail that can later be used to prove that a particular e-mail message was sent, that it was successfully delivered, and when and how.

Should a dispute ever arise, the dispute can be resolved through the receipt generated by the system because the receipt is so encoded that the operators of the system can determine the authenticity of the receipt as the product of the system. Thereafter, operators of the system can attest to the accuracy of the information contained in an authentic receipt, relying only on information contained in the receipt itself and without the need for the operators to preserve any record or copy of the information contained in the receipt.

In addition to these benefits, the receipts generated by the system may also be useful as evidence of the existence and authorship of such materials as might be transmitted through the system. Moreover, the system is easy to use, as the system can be used from any internet e-mail client program/MUA, so that there is no additional software required.

VII. FLOW DIAGRAM FOR VALIDATING A RECEIPT

FIG. 7 is a flow diagram illustrating an exemplary method for validating a receipt. In the event that the sender of a message should require evidence that an e-mail was sent and delivered (and/or read) the sender presents the receipt(s) corresponding to the message to the operators of the system in step 700. The operators of the system then, in step 702, detach and decrypt the document digital signature appended to the receipt. In step 703, the operators generate a hash of the balance of the document, including attachments.

In step 704, if the current hash value does not match the decrypted hash value, then the system generates a report stating that RPost cannot authenticate the receipt as

an accurate record of the delivery or the contents of the message described in the receipt.

If the decrypted hash is equivalent to the current hash of the message, the system can, as in step 706, warrant that the information contained in the body of the message is unchanged since the receipt passed through the system. If the original message contained no attachments, the system may now generate a report that warrants that the receipt is an accurate record of the message's contents and its delivery by the RPost server.

If the receipt reports that the original message contained attachments, then the receipt will also record the name and hash value of each attachment. In generating the receipt all attachments of the original message are attached unchanged to the receipt. Accordingly, the system will, for each such attached file, generate a hash of the attached file (708) and compare it to the hash value recorded in the body of the receipt (709).

If the calculated hash value of a file matches the value included in the receipt, the system can warrant that the file attached to the receipt is identical to that attached to the message as originally delivered. If the hashes do not match, then the system will report that it cannot warrant that the file attached to the receipt is identical to the file attached to the original message.

Having performed this calculation for each file attached to the original message, the system prepares a report which reports on the authenticity of the receipt and each of its attached files (710) or which reports the failure of validation (712).

Having completed its evaluation, the system will then append a copy of the receipt and all of its attachments to the report it has generated and send it via e-mail to the return address of the user who submitted the report for validation.

VIII. REGISTERING INBOUND EMAILS

FIG. 8 is a system diagram illustrating another embodiment of the invention in which incoming e-mails are made of record. In this embodiment, a message sender 60 sends an e-mail message 70. Sender's MTA 62 sends message 70 onto the internet as usual. However, in this embodiment RPost contracts with service subscriber/recipient 68 to make incoming e-mails of record. According to the agreement, RPost is designated with Network Solutions, Inc. (NSI) or other domain name authority as the mail recipient (MX server) for recipient 68. This causes the Domain Name Service (DNS) request performed by the sender's MTA 62 to return the IP address of RPost as the IP address for the recipient, which in turn causes sender's MTA 62 to send the e-mail message to RPost server 64. RPost server 64 acts as an SMTP, POP, POP3 or IMAP MTA (collectively, "POP mail server") for recipient 68. SMTP, POP and IMAP MTAs are governed by RFC 821, the SMTP protocol, RFC 1939 Post Office Protocol - Version 3 (which obsoleted RFC1725), and RFC 2060 IMAP (Internet Message Access Protocol) Version 4 rev 1 (which obsoleted RFC1730), which are hereby incorporated by reference.

RPost server 64 prepares a made-of-record version 74 of the original message 70, and places this made-of-record version 74 into recipient 68's in-box instead of, or in addition to, the original message 70. The made-of-record version may have all of the verification and informational features and options discussed earlier in connection with e-mail receipts. This information can include, but is not limited to: individual message digests for each of the message body and text, the to/from information, other header information, each attachment, an overall message digest and digital signature and message routing information and tags. Made-of-record version 74 of message 70 as shown in FIG. 6 includes the message body including the header information, an attachment, separate message digests for each, and a digital signature or encrypted message digest. The hash functions and encryption are performed using private

phrases or private keys known only to the operators of the system. The made-of-record version 74 is made available to recipient 68 for inspection or downloading through the recipient's MUA.

RPost server 64 can optionally send a confirming e-mail 72 to message sender 60. Confirmation message 72 can be a simple text message indicating that a message was received and made of record. Confirmation message 72 could also include a message such as, "Your e-mail message was received on March 24, 2000 at 2:05 p.m. The digital signature of the message was [128-bit digital signature]. For more information, visit our website at www.RPost.com." Alternatively, or additionally, confirmation message 72 could include all of the information contained in the made-of-record version 74.

Thus, the system may provide to message recipient 68 a receipt 74 or other verifiable confirmation that:

(1) the recipient received an e-mail message;

(2) the message was received at a certain time;

(3) the e-mail was addressed from a certain sender;

(4) the message purports to be delivered via a certain network route; and

(5) the e-mail message and its attachments had a specific content.

Accordingly, the system provides evidence, which may be attested to by the operators of the system, that particular electronic messages and documents were delivered to recipients having certain content and representing themselves as having come from certain senders.

IX. EXAMPLE OF MAKING OF RECORD IN-BOUND E-MAIL

FIG. 9 is a flow chart illustrating one example of making of record in-bound e-mail. In step 901, RPost server 64 receives a new e-mail message. In step 902, the system generates a hash/digital signature of the message's contents including the message's headers and attachments. Additionally, the system may generate a separate hash for each message attachment. In step 903, the system encrypts the hash(es) using an encryption key known only to the operators of the system. In step 904, the resulting encrypted hash(es) is then appended to the body of the message. Then, in step 905, the modified message may be made available for inspection or downloading through the recipient's MUA.

X. EXAMPLE OF VALIDATING A RECEIVED MADE-OF-RECORD E-MAIL MESSAGE

FIG. 10 is a flow chart of one example of validating a received made-of-record e-mail message. In step 1000, in the event that the recipient of a message should require evidence that an e-mail with a specific content was received at a particular time, the recipient can present a copy of the made-of-record version 74 (FIG. 8) of e-mail message 70 to the operators of the system for verification. To verify the message, in step 1001 the system detaches and decrypts the document digital signature appended to the message. In step 1002, the system generates a hash of the balance of the document, and one for each file attached to the message. In steps 1003 and 1004, the hashes are compared. If the document hash(es) matches the decrypted hash(es), then the message and its attachments have passed through the system and have not been altered since their delivery to the recipient.

Having determined that the e-mail is unaltered, the operators of the system can warrant that:

(1) the e-mail was received by the system at a certain time;

(2) the e-mail purported to arrive at the system via a certain internet route;

(3) the e-mail purported to be from a certain sender; and

(4) the e-mail and its attachments were delivered with the specific content they currently contain.

On the other hand, in step 1006, if the hash values do not match, then the operator cannot warrant that the e-mail is authentic, i.e., that the e-mail is an accurate version of an e-mail that was received by the system.

XI. HOW A BUSINESS UTILIZING ELECTRONIC TOOLS MAY USE THE INVENTION

FIG. 11 illustrates how the invention may be used by a business which utilizes electronic tools (an "e-business"). E-business 30 can utilize the system to make of record all incoming and outgoing e-mail messages from its customers 34. In this case, the system includes Post Office Protocol (POP) server 36 and Simple Mail Transfer Protocol (SMTP) server 38. For example, the e-business 30 can set up its website to e-mail forms to customers, and to forward queries and complaints 40 from customers 34. The made-of-record queries, complaints, orders, offers to purchase, and other information 46 are sent to the e-business 30 by the system. Receipts are then provided to the customers 34 via SMPT server 38. This way there is no question regarding whether or not the customer sent the communication and what it contained. Moreover, the e-business can set up a web site 32 through the RPost server so that every communication with the customers can be made of record. In other words, through the web site form data orders 42 and automated responses 44 can be made of record through the system server; furthermore, any confirmation, collections notices, customer support, and special offers 48 sent by the e-business to customers 34 can be made of record and the confirmation sent to the customer to eliminate arguments about

what was ordered, when, or by whom. If desired, identical receipts can be provided to both the customers 34 and to e-business 30. Alternatively, the functions of POP server 36 and SMTP server 38 may be combined in a single system server.

POP is a protocol used to retrieve e-mail from an e-mail server. Many e-mail applications (sometimes called e-mail clients) use the POP protocol, although some can use the newer Internet Message Access Protocol (IMAP). One version of POP, called POP2, requires SMTP to send messages. A newer version, POP3, can be used with or without SMTP. SMTP is a protocol for sending e-mail messages between servers. Many e-mail systems that send e-mail over the internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. E-mail servers may use a variety of protocols to communicate with the internet. Commonly used protocols include SMTP, POP3 and IMAP4. Mail readers are at the opposite end of the server. Since mail servers receive messages via SMTP, e-mail readers send e-mail to a mail server using SMPT. Likewise, since mail servers send messages using POP3 and optionally IMAP4, mail readers receive messages from mail servers by using the POP3 or IMAP4 protocol.

Although the above generally describes a system and method of verifying that an e-mail was sent and/or received, the invention disclosed and claimed in application 09/626,577 may apply to any electronic message that can be transmitted through an electronic message network or through any electronic gate. Electronic messages may include text, audio, video, graphics, data, and attachments of various file types. The methods and techniques taught herein can be programmed into servers and other computers, and computer programs implementing the invention can be written onto computer readable media including but not limited to CD ROMs, RAM, hard drives, and magnetic tape. E-mail made-of-record services according to the present invention can be bundled with internet service provider (ISP) services to provide a single

provider ISP solution to corporate and other institutional clients. Implementing the above-described invention is within the skill of the ordinary practitioner of the software arts.

XII. SYSTEM PROVIDING FOR AN AUTHENTICATION OF A MESSAGE TO A RECIPIENT

In the embodiments shown in Figures 1-11, systems and methods are disclosed for authenticating to a sender a message transmitted by a server on behalf of the sender to the recipient. The authentication relates to (a) the content and wording of the message, (b) the time for the transmission of the message by the server to the recipient and (c) the intermediate stations through which the message is transmitted by the server to the recipient and (d) the intermediate stations through which the validation of the receipt of the message by the recipient is transmitted to the server. The authentication may be provided by producing a digital signature of the message and a digital signature of the attachment(s) to the message, these attachment(s) illustratively relating to the actual events involving the message at each of the intermediate stations or relating to a composite of the factual events at all of the intermediate stations.

As will be appreciated, the server is generally paid by the sender. Because of this, the server generally acts as an agent of the sender. To provide for an authentication of the message and the related information to the sender, the server sends to the sender a copy of the message, a digital signature of the message, the attachment(s) including the history of the transmission of the message to the successive intermediate stations between the server and the recipient and a digital signature of this history. The digital history may relate to each intermediate station individually as a separate attachment or may relate to a single attachment involving all of the intermediate stations or any combination of the above. The server does not have to retain any of this information because the sender will provide this information to the server when the sender wishes to obtain an authentication.

When the sender wishes to authenticate the message and the transmission of the message from the server to the recipient, the sender transmits to the server all of the information that the server has previously transmitted to the sender. This includes the message, the digital signature of the message, the history of the transmission of the message to the intermediate station(s) between the server and the recipient and the digital signature of this history. The transmission history between the server and the recipient may be considered as a single attachment comprising all of the intermediate stations or may be considered as a plurality of attachments each relating to an individual one, or combination of, of the intermediate stations.

To authenticate the message, the server obtains a digital fingerprint (or digital digest) of the message and a digital fingerprint (or digital digest) from the digital signature of the message. The server then compares the two (2) digital fingerprints (or digital digests). If the two (2) digital fingerprints match, the server authenticates the message. To authenticate the transmission history between the server and the recipient, the server produces a digital fingerprint of an attachment comprising the composite transmission history of all the intermediate stations between the server and the recipient (including the server and the recipient) or the transmission history at each, or combinations, of the intermediate stations between the server and the recipient. The server also obtains a digital fingerprint (or digital digest) of the digital signature derived from the attachment or attachments. The server then compares the digital fingerprint(s) of the attachment(s) and the digital fingerprint(s) derived from the digital signature(s) of the attachment(s). If the digital fingerprint(s) match, the server authenticates the transmission file history. The authentication to the sender of the message transmitted from the server to the recipient and the attachments to the message is disclosed and claimed in application 09/626,577 (attorney's file RPOST-57228) filed in the USPTO on 07/27/00 by Dr. Terrance A. Tomkow and assigned of record to the assignee of record of this application.

In order to authenticate that the message from the sender was transmitted to the recipient, the server authenticates the message and also authenticates the transmission of the message from the server to the recipient through the intermediate stations. If one of the authentications is provided but not the other, the server may not provide an authentication either of the message or the transmission history of the message.

As will be appreciated, the history of the transmission of the message from the server through the intermediate stations to the recipient and then from the recipient through the same or different intermediate stations to the server is available when the authentication is provided to the sender, as disclosed and claimed in application 09/626,577. Sometimes, however, the recipient may desire a prompt authentication of the transmission of the message and the transmission history.

As will be appreciated, the transmission history available to provide such an authentication is relatively brief. Available information for the transmission history at the time of the message transmission to the recipient may constitute essentially only the identity of the sender, the identity of the server, the identity and internet address of the recipient and the time for the transmission of the message from the server to the recipient.

Figure 12 schematically shows a system for authenticating a message to a recipient, and the transmission history of the message, from the server to the recipient. The system shown in Figure 12 is directed to the transmission of a court order from a court to an attorney for one of the parties in a lawsuit. When the attorney receives the message electronically as through the internet, the attorney may attempt to authenticate promptly the court order and the transmission of the court order. This may be particularly important to the attorney since the court order may direct the attorney to file a specified document within 24 hours or 48 hours in the court.

It will be appreciated that the example shown in Figure 12 is only one of a countless number of different examples that can be provided. For example, it may relate to all types of contractual matters where a first party in a proposed contractual

relationship with a second party may be proposing particular contractual terms to a second party and may be requesting a prompt acceptance or rejection of these terms. Under such circumstances, the second party may request prompt confirmation of the terms that the second party has received and may request prompt confirmation that the first party has submitted these terms to the second party.

As indicated previously, Figure 12 shows on a schematic basis a system and a flow chart, generally indicated at 1200, in which a court 1202 issues an order or a ruling to an attorney in a lawsuit in which the attorney is representing one of the parties in the suit. As a first step indicated at 1202, the court 1202 issues the order, preferably electronically (e.g. via the internet) by (R)egistered e-mail™. Messages transmitted and received by registered e-mail are disclosed and claimed in co-pending application 09/626,577 (attorney-docket RPOST-57228) filed by Dr. Terrance A. Tomkow for a SYSTEM FOR, AND METHOD OF, AUTHENTICATING DELIVERY AND INTEGRITY OF ELECTRONIC MESSAGES on July 27, 2000 and assigned of record to the assignee of record of this application.

As a first step in the method 1200 shown in Figure 12, a U.S. court 1202 transmits a notification (e.g. a court order) in a lawsuit to a server 1204. The transmission from the U.S. court to the server 1204 is indicated at 1206. The notification may be by e-mail in accordance with the system and method claimed in co-pending application 09/626,577. The server 1204 then transmits the notification to an attorney 1208 who represents one of the parties in the lawsuit. This transmission is indicated at 1210. It may be by e-mail. The server 1204 also transmits a delivery receipt to the U.S. court to indicate that the notification has been delivered (or not delivered) to the attorney 1208 and the time of the delivery. This delivery receipt is indicated at 1212 in Figure 12. The delivery 1212 may be a registered receipt. The U.S. court retains a copy of this notification to indicate the court order transmitted to the attorney 1208 and the time of the transmission and to indicate whether or not the

notification has been received by the attorney 1208 and also whether or not the notification has been opened by the attorney's client.

The attorney 1208 can verify the authenticity of the notification by forwarding it to the server 1204. See 1214. The forwarding can be to a special website at the server 1204 such as "verifyatrpost.net". By forwarding the notification to verifyatrpost.net, the attorney 1208 will receive an authentication receipt which will authenticate the notification and the time of transmission of the notification to the attorney 1208.

The attorney 1208 can also forward the notification to any third party. The third party can then request authentication of the notification in the same manner as discussed in the previous paragraph with respect to authentication of the notification to the attorney 1208. In this way, the authentication capability is retained by the attorney and is transferred to other parties even when the attorney 1208 forwards the notification to the third party.

The sophistication of the authentication capability can be enhanced by the server 1204 from that discussed above. The server can create a digital signature of the court order. The attorney 1208 can then transmit the message to the website verifyatrpost.net. The website can then produce a digital fingerprint (or digital digest) of the order transmitted by the attorney 1288 to the server 1204 and a digital fingerprint from the digital signature of the order from the court 1202. When the two (2) digital fingerprints match, the server 1204 can authenticate the message.

When the server 1204 transmits the notification to the attorney 1208, the server knows certain information such as the identity of the U.S. court, the identity and address of the recipient and the time of the transmission of the message to the recipient. This certain information may also include the identity of the server. The court order and the certain information specified in this paragraph may be transmitted to the attorney 1208. To obtain an authentication of this information, the attorney 1208 forwards this information to the website verifyatrpost.net. In addition to the authentication discussed in the previous paragraph, the server 1204 can then verify the

certain information such as the identity of the sender, the identity of the server, the identity and address of the recipient and the time of the transmission of the notification from the server to the recipient. This certain information can be compared with corresponding information at the server 1204 to provide an authentication at the server 1204 in addition to the authentication of the court order.

Instead of providing a digital signature of only the notification (court order), the server 1204 can also produce a digital signature of the notification and the certain information such as the identity of the sender, the identity of the server and the identity and address of attorney 1208. The server 1204 can then transmit the notification and the certain information to the attorney 1208. When the attorney 1208 desires to obtain an authentication, the attorney forwards the notification and the certain information to the website verifyatrpost.net at the server 1204. The server 1204 then produces a digital fingerprint from the notification and the certain information from the attorney 1208 to the server 1204 and a digital fingerprint from the digital signature produced by the server 1204. When the two (2) digital fingerprints match, the server 1204 is able to provide an authentication to the attorney 1208.

In addition to providing a digital signature of the notification, the server 1204 may also provide a digital signature of the certain information such as the identity of the sender, the identity and address of each of the server 1204 and the attorney 1208 and the time of the transmission from the server to the attorney. The server 1204 may then transmit to the attorney 1208 the notification, the digital signature of the notification and the certain information. To obtain an authentication, the attorney 1208 forwards to the server 1204 at verifyatrpost.net the notification and the certain information. The server 1204 then produces digital fingerprints of the notification with the certain information and digital fingerprint(s) of the digital signature(s). The server compares the digital fingerprints of the notification and the digital fingerprint of the notification and compares the digital fingerprints of the certain information. When

each of the comparisons matches, the server 1204 provides an authentication to the attorney 1208.

The server 1204 also transmits to the court 1202 the notification, the digital signature of the notification and the transmission history between the servers 1204 and the attorney 1208. As previously indicated, the transmission history may include the intermediate stations between the server 1204 and the attorney 1208 and may also include the times of transmission to the intermediate stations. If the server 1204 provides a digital signature of this transmission, the server 1204 may also transmit this digital signature to the court 1202. When the attorney 1208 wishes to authenticate the message and the time of transmission of the message from the server 1204 to the attorney 1208, the court 1202 may transmit to the server what the court has previously received from the server. The server 1204 may then use this information, in the manner described above, to authenticate to the attorney 1208 the notification and the time of transmission of the notification from the server to the attorney 1208.

Another method of authenticating to a recipient also may consist of the following steps performed at the sender's mail client or mail transport agent.

1. A digital digest is taken of each attachment of the message.

2. A copy of the message is made, stripped of any file attachments and compressed or hashed.

3. The digital digests and the compressed body of the message are combined with information identifying the sender and are encrypted as an alphanumeric string.

4. A digital digest of this string is taken.

5. A file is prepared which contains, in HTML format, information identifying the sender and instructions on how to validate the

message. The instructions invite anyone who wishes to confirm the integrity of the message to forward a copy of the message, with all its attachments in place, to an email address. The encrypted string is concealed within the file in an HTML comment field. Because the file does not contain copies of the original message's attachments, it may be quite small even though the message is large.

6. The HTML file is attached to the message and the message is sent.

On receiving this message, any recipient wishing to confirm the authenticity of the message can do so by forwarding it to the indicated address. When the forwarded message is delivered to the address, the sender of the original message or an agent of the sender can perform the following steps.

1. The encrypted string is extracted from the HTML attachment and decrypted.

2. Digital digests of the other file attachments of the message are computed and compared to the digital digests extracted from the encrypted string.

3. If the file digests are equivalent, indicating that the file attachments have not been changed, the body of the original message is extracted from the HTML file. Its digital digest is compared with the digest stored in the HTML file. If the digests are equivalent the compressed message body is decompressed and saved to a new file.

4. The file attachments of the submitted message are detached and attached to the new file. The new file is now a highly accurate reconstruction of the original message.

5. The reconstructed message is now attached to a message that identifies the original sender of the message and reports that a reconstruction of the original message is attached. This authenticating message is returned to the reply-address of the forwarded message.

If the digital digests indicate that either the file attachments, or the compressed string, have been altered, a message reporting a failure of authentication is returned to the reply-address of the forwarded message.

The system of "digitally sealing" a message is universal, non-fragile and resilient.

It is universal insofar as any recipient of the message will be able to authenticate the message simply by forwarding it to the authentication address.

The system is not fragile since: so long as the message's file attachments are not corrupted, the message may be changed in many ways without interfering with its accurate reconstruction.

The system is resilient in the sense that an accurate copy of the original message can be reconstructed despite significant corruption of the message.

Figures 13and 14 illustrate an embodiment of the system where the digital sealing operations are performed at a Mail Transport Agent removed from the sender.

Figure 13 illustrates the sealing of a message by the server 1204:

When the message is delivered to the server 1204 via an authenticated SMTP connection 1301, the system consults a database 1302 to recover identifying information about the sender. This information is stored in a string 1303.

The file attachments of the message may be hashed as at 1304 and attached to the string 1303.

A copy is made of the original message as at 1305 and stripped of its file attachments 1306.

The result 1307 is appended to the string 1303. String 1303 is hashed and the result is appended to the string 1303.

The string 1303 is digitally compressed or hashed as at 1008 and encrypted as at 1309 and then attached to an HTML file 1310, concealed in a comment. The comment is indicated in the file 1318 Identifying information about the sender is included in plain text in 1310 as well as instructions about how to authenticate the message.

The HTML file is then attached as at 1311 to the original message and the result is sent to the message's addressee as at 1312.

Figure 14 illustrates the process of authentication of a digitally sealed message such as indicated at 1312 in Figure 13.

To authenticate the message the recipient forwards a copy to the server as at 1313.

The digital seal file is detached from the message as at 1314 and the embedded encrypted string 1315 is extracted, decrypted as at 1316 and decompressed as at 1317.

A hash of the string, less its embedded hash, is taken as at 1318. The result is compared as at 1319 to the embedded hash. If they are not equivalent the system sends a message to the submitter saying that the message cannot be authenticated because it has become corrupted. (See 1320.)

If the hashes are equivalent (1321) the system hashes the file attachments of the original message 1322 and compares these to the hashes stored in 1315. If these are not equivalent the system returns a failure notification 1320.

If the files are equivalent the system creates a new email message as at 1324 from the original message text (less file attachments) stored in 1315.

The file attachments of the submitted message are attached (see 1325) to the message 1324. The message 1324 is now an accurate reconstruction of the original message.

The reconstructed message 1324 is now attached as at 1326 to a message which reports successful authentication of submitted message 1327 and the result is sent to the submitter 1328.

The term "recipient" is used in the claims to indicate the receiver of the message and attachments provided through the server from the sender. The term "recipient" is also intended in the claims to include any agent of the receiver with respect to the message and the attachment(s). Such agent may include a Mail Transport Agent of the

recipient. In the claims, the term "digital digest" or "digital fingerprint" of a message can be considered to be a hashing or compression of the message. In the claims, the term "digital signature" of a message can be considered to be an encryption of a digital digest or a digital fingerprint. In the claims, the term "message" can be considered to be all or a portion of the message. In the claims, the term "attachment" can be considered to be all or a portion of the history of the transmission of the message through the interim stations between the server and the recipient. the term "attachment" can also be considered in the claims to include a plurality of all attachments such as are provided by a plurality of interim stations between the server and the recipient.

Although the present invention has been described in detail with regard to the preferred embodiments and drawings thereof, it should be apparent to those of ordinary skill in the art that various adaptations and modifications of the present invention may be accomplished without departing from the spirit and the scope of the invention. Accordingly, it is to be understood that the detailed description and the accompanying drawings as set forth hereinabove are not intended to limit the breadth of the present invention.